Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1.   (withdrawn) A method of mirroring security processors comprising the steps of:

generating information for a first security processor;

repeatedly sending the information to a second security processor in accordance with the first security processor processing at least one packet.

2.   (withdrawn) The method of claim 1 wherein the sending step comprises sending the information from the first security processor to the second processor.

3.   (withdrawn) The method of claim 1 wherein the generating step comprises generating the information in the first security processor.

4.   (withdrawn) The method of claim 1 further comprising the step of generating at least one packet including the information, wherein the sending step comprises sending the at least one packet over a packet network.

5.   (withdrawn) The method of claim 1 wherein the sending step further comprises sending the information over a dedicated link between the first security processor and the second security processor.

6.   (withdrawn) The method of claim 5 wherein the dedicated link comprises an Ethernet link.

7.   (withdrawn) The method of claim 1 wherein the sending step comprises repeatedly sending the information on a per-packet basis.

8.   (withdrawn) The method of claim 1 wherein the sending step comprises repeatedly sending the information at intervals according to at least one sequence number.

9.   (withdrawn) A method of mirroring security processors comprising the steps of:

generating security association information for a first security processor; and

repeatedly sending the security association information to a second security processor in accordance with the first security processor processing at least one packet.

10.   (withdrawn) The method of claim 9 wherein the information comprises at least one security association sequence number.

11.   (withdrawn) The method of claim 9 wherein the information comprises at least one security association byte count.

12.   (withdrawn) The method of claim 9 wherein the sending step further comprises repeatedly sending the security association information on a per-packet basis.

13.   (withdrawn) The method of claim 9 wherein the sending step further comprises repeatedly sending the security association information at intervals according to at least one sequence number.

14.   (withdrawn) The method of claim 9 further comprising the step of generating at least one packet including the security association information, wherein the sending step comprises sending the at least one packet.

15.   (withdrawn) The method of claim 9 further comprising the step of generating at least one packet including the security association information, wherein the sending step comprises sending the at least one packet over a packet network.

16.   (withdrawn) The method of claim 9 wherein the sending step further comprises sending the information over a dedicated link between the first security processor and the second security processor.

17.   (withdrawn) The method of claim 16 wherein the dedicated link comprises an Ethernet link.

18.   (currently amended) A method of providing redundancy in a security processing system comprising the steps of:

establishing a first secure packet flow through a first mirrored security processor;

updating security association information associated with the first secure packet flow;

establishing a second secure packet flow through a second ~~mirrored~~

security processor;

updating security association information associated with the second

secure packet flow;

sending the updated security association information associated with

the first secure packet flow from the first ~~mirrored~~ security processor to the second

security ~~mirrored~~ processor in a first update packet ~~having a custom routing header~~

~~configured to allow routing of the first update packet through mirrored security~~

~~processors, wherein first update packet is sent~~ when a sequence number in the security

association information associated with the first secure packet flow reaches a first

predefined value ~~at a first predefined interval~~;

sending the updated security association information associated with

the second secure packet flow ~~for~~ from the second ~~mirrored~~ security processor to the

first ~~mirrored~~ security processor in a second update packet ~~having a custom routing~~

~~header configured to allow routing of the second update packet through mirrored~~

~~security processors, wherein second update packet is sent~~ when a sequence number in

the security association information associated with the second secure packet flow

reaches a second predefined value ~~at a second predefined interval~~; and

storing the updated security association information associated with the

first secure packet flow and the updated security association information associated

with the second secure packet flow in the first ~~mirrored~~ security processor and in the

second ~~mirrored~~ security processor.

19.   (currently amended) The method of claim 45 wherein the rerouting

step is in response to a failure of packet flow through the first ~~mirrored~~ security

processor.

20.   (canceled)

21.   (currently amended) The method of claim 18 wherein ~~the the custom~~

~~routing header comprises a at least one sequence number, wherein~~ the sequence

number <u>in the security association information associated with the first secure packet</u>

<u>flow</u> is incremented when ~~an update~~ <u>a</u> packet <u>in the first secure packet flow</u> is

received from or transmitted to a network.

22.   (currently amended) The method of claim 18 wherein <u>the security</u>

<u>association information associated with the first secure packet flow</u> ~~the custom~~

~~routing header~~ comprises a at least one byte count.

23-24. (canceled)

25. (currently amended) The method of claim 18 further comprising the step

of generating at least one configuration packet including the security association

information <u>associated with the first secure packet flow</u>, wherein sending the updated

security association information from the first ~~mirrored~~ security processor to the

second ~~mirrored~~ security processor comprises sending the at least one configuration

packet.

26. (currently amended) The method of claim 18 further comprising the step of sending, by a host processor, configuration information to the first ~~mirrored~~ security processor and the second ~~mirrored~~ security processor.

27. (currently amended) The method of claim 18 further comprising the step of sending, by a host processor, security association configuration information to the first ~~mirrored~~ security processor and the second ~~mirrored~~ security processor.

28. (canceled)

29. (currently amended) The method of claim 18 further comprising the steps of:

defining a quantity to adjust [[a]] the sequence number in the security association information associated with the first secure packet flow;

defining an interval at which to update the security association information associated with the first secure packet flow; and

determining whether to send the security association information associated with the first secure packet flow to the second ~~mirrored~~ security processor according to a comparison of [[a]] the sequence number with the interval.

30. (currently amended) The method of claim 29 further comprising adding the quantity to the sequence number before sending the security association information associated with the first secure packet flow to the second ~~mirrored~~ security processor.

31-33. (canceled)

34.   (currently amended) The method of claim 18 further comprising the step of sending replay window information to the second ~~mirrored~~ security processor.

35.   (withdrawn) A security processing system, comprising:

a first security processor for processing packets and for updating security association information associated with the packets, the first security processor comprising at least one MAC for sending updated security association information over a packet network; and

a second security processor for receiving the updated security association information over the packet network.

36.   (withdrawn) The security processing system of claim 35 further comprising at least one host processor connected to the first security processor and the second security processor for terminating or initiating the packets.

37.   (withdrawn) The security processing system of claim 36 wherein the at least one host processor changes the routing of packet flow by either routing the packets to the second security processor instead of the first security processor.

38.   (currently amended) A security processing system, comprising:

a first ~~mirrored~~ security processor configured to process a first packet flow, update security association information in response to the first packet flow, and send the updated security association information associated with the first packet flow in a first update packet <u>when a sequence number in the security association information associated with the first packet flow reaches a first predefined value</u>

~~having a custom routing header configured to allow routing of the first update packet~~

~~through mirrored security processors~~; and

a second ~~mirrored~~ security processor configured to process a second

packet flow, update security association information in response to the second packet

flow, and send the updated security association information associated with the

second packet flow in a second update packet <u>when a sequence number in the security</u>

<u>association information associated with the second packet flow reaches a second</u>

<u>predefined value</u> ~~having a custom routing header configured to allow routing of the~~

~~second update packet through mirrored security processors~~,

wherein the first ~~mirrored~~ security processor is further configured to

send the updated security association information in response to the first packet flow

to the second ~~mirrored~~ security processor at a first predefined interval and the second

~~mirrored~~ security processor is further configured to send the updated security

association information in response to the second packet flow to the first ~~mirrored~~

security processor.

39.   (currently amended) The security processing system of claim 46

~~further comprising~~ <u>wherein the</u> at least one host processor <u>is</u> connected to ~~the~~ at least

one switch for terminating or initiating the first packet flow and the second packet

flow.

40.   (currently amended) The security processing system of claim 39

wherein the at least one host processor changes the routing of packet flow by either

routing the first packet flow to the second ~~mirrored~~ security processor instead of the

first ~~mirrored~~ security processor or routing the second packet flow to the first

~~mirrored~~ security processor instead of the second ~~mirrored~~ security processor.

41.   (currently amended) The security processing system of claim 40

wherein the change in the routing is in response to a failure of the first packet flow

through the first ~~mirrored~~ security processor or the second packet flow through the

second ~~mirrored~~ security processor.

42.   (canceled)

43.   (currently amended) The security processing system of claim <u>46</u> [[47]]

wherein the at least one host processor routes the first packet flow to the second

security ~~mirrored~~ processor instead of the first security processor.

44.   (currently amended) The security processing system of claim <u>43</u> [[48]]

wherein the at least one host processor routes the second packet flow to the first

~~mirrored~~ security processor instead of the second ~~mirrored~~ security processor.

45.   (currently amended) The method of claim 18, further comprising:

            rerouting the <u>first</u> secure packet flow to flow through the second

~~mirrored~~ security processor instead of the first ~~mirrored~~ security processor

46.   (currently amended) The security processing system of claim 38,

further comprising:

            at least one host processor for establishing [[a]]] first packet flow to the

first ~~mirrored~~ security processor and [[a]] <u>the</u> second packet flow to the second

~~mirrored~~ security processor [[;]] <u>.</u>